

Prior Art Information List

| | |
|---------------|----------|
| Your case No. | |
| Our case No. | FUT01013 |

| Inventor, Patent Number, Country Author, Title, Name of Document | Issue date | Concise Explanation of the Relevance (indication of page, column, line, figure of the relevant portion) |
|--|------------|---|
| Inventor: MASUOKA RYUSUKE etal Publication Number: 08-044643 | 16.02.1996 | |
| Inventor: ISOMICHI HIROYO etal Publication Number: 2000-003334 | 07.01.2000 | |
| Interface '95 No.9 Chapter 5: The functional details of the multipurpose proxy server DeleGate – Access / routing control and Protocol conversion (Yutaka Sato) | 01.09.1995 | PP130—146 (abstract) |

Best Available Copy

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-044643
 (43)Date of publication of application : 16.02.1996

(51)Int.Cl.

G06F 13/00
 G06F 13/00
 G06F 12/00

(21)Application number : 06-175125
 (22)Date of filing : 27.07.1994

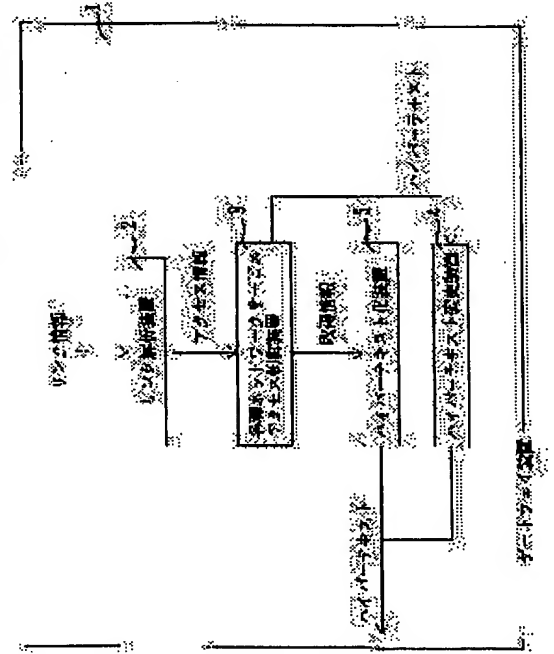
(71)Applicant : FUJITSU LTD
 (72)Inventor : MASUOKA RYUSUKE
 OKADA HIROYUKI
 SUEMATSU NOBUAKI

(54) GATEWAY DEVICE

(57)Abstract:

PURPOSE: To perform access to an external data base while keeping transparency to a user without using any special client and sacrificing security by using a hypertext by providing a hypertext changing device for outputting the hypertext after the change of link information.

CONSTITUTION: A link analyzing device 2, that receives the link information, changes that information into access information and dispatches it to various network service access controllers 3. Based on this access information, the various access controllers 3 access various network servers and acquire the information designated by the access information. When this acquired information is the hypertext, it is dispatched to a hypertext changing device 4. According to a processing method to which the link information in the acquired information is applied, the hypertext changing device 4 outputs the hypertext reloaded (changed) so as to access this gateway device 1, the other gateway device or the server.



LEGAL STATUS

[Date of request for examination]
 [Date of sending the examiner's decision of rejection]
 [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
 [Date of final disposal for application]
 [Patent number]
 [Date of registration]
 [Number of appeal against examiner's decision of rejection]
 [Date of requesting appeal against examiner's decision of rejection]
 [Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-44643

(43) 公開日 平成8年(1996) 2月16日

| (51) Int.Cl. ⁶ | 識別記号 | 序内整理番号 | F I | 技術表示箇所 |
|---------------------------|---------|---------|-----|--------|
| G 0 6 F 13/00 | 3 5 3 C | 7368-5E | | |
| | 3 5 5 | 7368-5E | | |
| 12/00 | 5 4 7 H | 7623-5B | | |

審査請求 未請求 請求項の数 9 O L (全 14 頁)

(21) 出願番号 特願平6-175125

(22) 出願日 平成6年(1994) 7月27日

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中1015番地

(72) 発明者 益岡 竜介

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

(72) 発明者 岡田 浩之

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

(72) 発明者 末松 伸朗

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

(74) 代理人 弁理士 山谷 皓榮 (外1名)

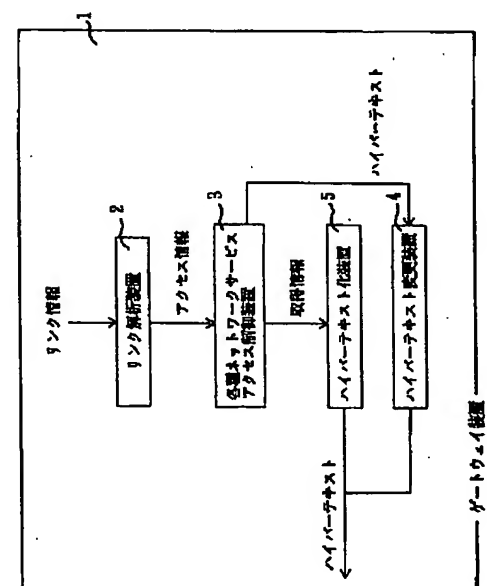
(54) 【発明の名称】 ゲートウェイ装置

(57) 【要約】

【目的】 ハイパーテキストを用いることにより、特別なクライアントを用いずに、しかもセキュリティを犠牲にせず、ユーザに対して透明なままで外部のデータベースにアクセス可能とすることを目的とする。

【構成】 ハイパーテキストのリンクの置き換えをするリンク置き換え処理装置と、リンクの変更をするリンク変更処理装置とをハイパーテキスト変更装置4に備え、リンク置き換え処理装置がハイパーテキストを受け取ると、リンク変更処理装置でリンク情報を特定の処理手段に従って変更した後、リンク置き換え処理装置がリンク情報変更後のハイパーテキストを出力するようにする。

本発明の原理説明図



1

【特許請求の範囲】

【請求項1】 ハイパーテキストのリンクの置き換えをするリンク置き換え処理手段と、
リンクの変更をするリンク変更処理手段とをハイパーテキスト変更装置に備え、
リンク置き換え処理手段がハイパーテキストを受け取ると、リンク変更処理手段でハイパーテキスト中のリンク情報を特定の処理手段に従って変更した後、
前記リンク置き換え処理手段が前記リンク情報変更後のハイパーテキストを出力するようにするハイパーテキスト変更装置を備えることを特徴としたゲートウェイ装置。

【請求項2】 ハイパーテキスト化するハイパーテキスト化処理手段と、
リンクを生成するリンク設定処理手段とをハイパーテキスト化装置に備え、
ハイパーテキスト化処理手段で取得情報をハイパーテキスト化し、
リンク設定処理手段でリンク情報を特定の処理手段に従って変更した後、
前記ハイパーテキスト化処理手段が前記リンク情報変更後のハイパーテキストを出力するハイパーテキスト化装置を備えることを特徴としたゲートウェイ装置。

【請求項3】 前記リンク情報を変更する特定の処理手段として、再び同じゲートウェイにアクセスする情報を加える手段を設けることを特徴とした請求項1又は2記載のゲートウェイ装置。

【請求項4】 前記リンク情報を変更する特定の処理手段として、再び同じゲートウェイ或いは他のゲートウェイにアクセスする情報を加える手段を設けることを特徴とした請求項1又は2記載のゲートウェイ装置。

【請求項5】 前記リンク情報を変更する特定の処理手段として、他のサーバにアクセスする情報を設ける手段を備えることを特徴とした請求項1又は2記載のゲートウェイ装置。

【請求項6】 リンク情報を受け取り、リンク情報を解析するリンク解析装置と、
該リンク解析装置からのアクセス情報をもとに、サーバにアクセスし、情報を取得する各種ネットワークサービスアクセス制御装置と、
前記取得情報がハイパーテキストの場合ハイパーテキストのリンク情報を特定の処理手段に従って変更するハイパーテキスト変更装置と、
前記取得情報がハイパーテキストでない場合ハイパーテキスト化すると共にリンク情報を特定の処理手段に従って変更するハイパーテキスト化装置とを備えることを特徴としたゲートウェイ装置。

【請求項7】 前記リンク情報を変更する特定の処理手段として、再び同じゲートウェイにアクセスする情報を加える手段を設けることを特徴とした請求項6記載のゲ

2

ートウェイ装置。

【請求項8】 前記リンク情報を変更する特定の処理手段として、再び同じゲートウェイ或いは他のゲートウェイにアクセスする情報を加える手段を設けることを特徴とした請求項6記載のゲートウェイ装置。

【請求項9】 前記リンク情報を変更する特定の処理手段として、他のサーバにアクセスする情報を設ける手段を備えることを特徴とした請求項6記載のゲートウェイ装置。

10 【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明はハイパーテキスト中のリンクを変更する、あるいはハイパーテキストによるゲートウェイを実現する装置に関する。

【0002】 近年、ネットワーク上に分散したデータベースおよび、それらにアクセスするためのクライアントが各種出てきている。それらをサポートするネットワークのプロトコルには、ローカルファイルシステム (LOCAL FILE SYSTEM)、エフティピ (FTP)、インタネットニュース (INTERNET NEWS)、テルネット (TELNET)、ウェイズ (WAIS)、ゴファ (GOPHER)、ワールドワイドウェブ (WWW: World Wide Web) のHTTP (Hypertext Transfer Protocol) などがある。特にWWWでは直接、或いはゲートウェイを使って他のプロトコルを使うサーバにアクセスして、それらの結果を最終的にハイパーテキストにしてユーザに表示している。

【0003】 さてこのようにいろいろな情報が簡単に手に入るが、会社などの情報のセキュリティを守る必要のある組織では外部とのアクセスを制限しているところが多い。しかし一方でネットワーク上の各種データベースが充実するにつれ、それらのデータに簡単にアクセスすることが要求されている。

【0004】 このため、必要なデータベースのセキュリティを守りながら、ユーザに対して外部のデータベースに対しても内部のデータベースにアクセスするのと同様のアクセス、即ち透明なアクセスを実現することが要望されている。

【0005】

40 【従来の技術】 まず、ここで使用する言葉の定義をする。サーバ (server) は、データベースを持ち、特定のプロトコルを使ってアクセスしてきたクライアントに対して情報を提供するものである。

【0006】 クライアント (client) は、特定のプロトコルを使ってサーバが持つ情報を取ってくるものであり、通常ソフトウェアで実現されているものである。プロトコル (protocol) は、コンピュータとコンピュータがある目的 (例えばファイルをやりとりするなど) を持って通信しあう際の取り決めである。

50 【0007】 ハイパーテキスト (hypertext) は、情報

を提示するための一方法であり、文書中のいくつかの言葉がリンクになっており、それらの言葉が選ばれるとそのリンクが指す先の文書が表示されるようになっていく。そして、リンクの指す先の文書はハイパーテキスト、通常のテキスト、静止画、動画、音、その他何でも構わないものである。

【0008】リンク (link) は、言葉が指す文書にどうすればアクセスできるかを示した文字列のことであり、このリンクはハイパーテキストをフォーマットとして表示するクライアントでは通常ユーザから見えないように隠されている。例えば文字列に「どのプロトコルで、どのマシンのどのファイルにアクセスする」といった情報が含まれているものである。

【0009】従来にも、組織の外部のネットワークに設けられたサーバに組織の外部のネットワークのコンピュータではなく、組織内部のコンピュータから直接組織外部のサーバにアクセスする方法があった。

【0010】この場合に組織のセキュリティを確保する方法は、通常次のようなものがある。組織の外部のネットワークと内部のネットワークをルータ (router) で接続する。そして、このルータではそこを通れるプロトコルの種類とその方向を制限し、それを防壁 (firewall) として組織内部のセキュリティを確保するものである。

【0011】図9、図10は、従来例の説明図であり、以下、図9の従来例1に基づいて説明する。図9において、組織内部のネットワーク11には、ユーザ13が使用するコンピュータ14が設けてある。組織の外部のネットワーク12には、コンピュータ16と各種のプロトコルであるFTP、TELNET、WAIS、GOPHER、HTTPをもつサーバ (図示せず) が接続されている。そして、組織内部のネットワーク11と外部のネットワーク12は、限られたプロトコル (TELNET、FTP) しか通れないルータ15を介して接続されている。

【0012】このような環境の下で外部にアクセスを確保する方法は、組織の外部のネットワーク上の何台かの (図では1台を示す) コンピュータ16に、組織内部から外部のネットワークに用意されたコンピュータ16にTELNET、FTPなどを使ってアクセスできるようにしておく。これにより組織内部のネットワーク上に置いてあるコンピュータ14を使ってユーザ13が外部にアクセスする必要がある場合には、まず、組織内部のマシンであるコンピュータ14から、例えばTELNETでルータ15を通して組織外部のネットワーク12に用意されたコンピュータ16に入り、次に、その他の組織外部のマシンにコンピュータ16で変更された各種のプロトコルでアクセスして情報を得るようにしていた。

【0013】また、組織内部のセキュリティを確保しながら組織外部にアクセスを確保する他の方法として図10の従来例2があった。以下、図10に基づいて説明す

る。図10中、図9と同じものは同じ符号で示す。

【0014】図10において、新たにZZZというプロトコル (ZZZは仮の名前である) がルータ15を通れるようにする。そして、ルータ15を通れない通常のプロトコル例えばGOPHER、HTTPなどを使うクライアントであるコンピュータ14を変更して、ZZZのプロトコルを使う特殊なクライアント17とする。また、組織の外部のネットワーク12にゲートウェイ装置であるZZZのサーバ18を設ける。

10 【0015】組織内部のネットワーク11からユーザ13が外部にアクセスする必要がある場合、まず、ZZZのプロトコルを使って、ルータ15を通り外部のネットワーク12上のコンピュータ16上で走っているZZZサーバにアクセスする。次に、ZZZサーバ18がクライアント17の代わりに外部のネットワーク12にある例えばGOPHER、HTTPなどのサーバにアクセスし、クライアント17にその情報を返していた。

【0016】

20 【発明が解決しようとする課題】 上記従来のものにおいては、次のような課題があった。従来例1のように、外部のネットワーク12上のコンピュータ16を使う方法は、1度コンピュータ16の内部に入る例えばログインの手続などのため非常に手間がかかる。また、例えば自分の使うコンピュータ14からグラフィカル表示をするウィンドウ対応のクライアントを使おうと思ってもルータ15がTELNET等のキャラクタベース (character base) のプロトコルしか通さないので使用できないなど、組織内部のネットワーク上にある自分の使うコンピュータ14から、直接決まったプロトコルを使って、外部のサーバと通信する必要がある場合、一般のクライアントを使えないという欠点があった。

30 【0017】また、従来例2のように、プロトコルZZZのような特殊なクライアント17を使う方法は、自分の使うコンピュータからクライアントが使えるが、使おうとするクライアントはそのまま使えず、使いたい通常のプロトコルであるZZZを使って通信するような特別なクライアント17に変更する必要があった。

40 【0018】本発明は、ハイパーテキストを用いることにより特別なクライアントを用いずに、セキュリティを犠牲にせず、ユーザに対して透明なままで、外部のデータベースにアクセスすることを目的とする。

【0019】

50 【課題を解決するための手段】 本発明は、上記課題を解決するため次のように構成した。図1は、本発明の原理説明図であり、図1において、ゲートウェイ装置1には、リンク情報を解析するリンク解析装置2、各種ネットワークサーバにアクセスして指定された情報を取得する各種ネットワークサービスアクセス制御装置3、取得情報のハイパーテキストを変更するハイパーテキスト変

更装置4、取得情報をハイパーテキスト化するハイパーテキスト化装置5が設けてある。

【0020】

【作用】上記構成に基づく本発明の作用を、図1に基づいて説明する。まず、リンクの情報をリンク解析装置2が受け取る。リンク解析装置2は、リンクを解析し、アクセスするための情報であるアクセス情報に変更して各種ネットワークサービスアクセス制御装置3に渡す。各種ネットワークサービスアクセス制御装置3は、このアクセス情報を元に各種ネットワークサーバにアクセスし、アクセス情報に指定された情報を取得する。この取得した情報である取得情報が、ハイパーテキストである場合にはハイパーテキスト変更装置4に渡す。ハイパーテキスト変更装置4は、取得情報の中のリンク情報が与えられた処理方法に従って、このゲートウェイ装置1あるいはその他のゲートウェイ装置あるいはその他のサーバにアクセスするように書き換え（変更）られたハイパーテキストを出力するものである。

【0021】前記各種ネットワークサービスアクセス制御装置3の取得情報がハイパーテキストでない場合には、その取得情報をハイパーテキスト化装置5に渡す。これにより、ハイパーテキスト化装置5は、取得情報の中のリンク情報がこのゲートウェイ装置1あるいはその他のゲートウェイ装置あるいはその他のサーバにアクセスするように設定したハイパーテキストを出力することになる。

【0022】このような、ゲートウェイ装置1を外部のネットワーク12上に設けると組織内部のネットワーク上のコンピュータから通常のハイパーテキストのクライアントを使って、しかもセキュリティを犠牲にすることなく、外部のネットワーク上にあるリソース（資源）にアクセスできるようになる。

【0023】

【実施例】本発明の実施例を図2～図8に基づいて説明する。図中、図1と同一のものは同一の符号で示してある。

【0024】図2は、本発明の実施例におけるゲートウェイ装置の構成図であり、ネットワーク制御装置7は、ネットワークを使って行う通信の制御をするものである。アクセス監視・制御装置6は、ネットワーク制御装置7を監視し、アクセスがあったかを監視している。

【0025】アクセス監視・制御装置6は、他のクライアントからアクセスがあると、そのクライアントから与えられたリンク情報をゲートウェイ装置1に渡す。ゲートウェイ装置1は、通常とは異なるリンクを持ったハイパーテキストをアクセス監視・制御装置6に返す。これにより、アクセス監視・制御装置6は、ネットワーク制御装置7を制御してアクセスしてきたクライアントにそのハイパーテキストを返すものである。

【0026】この際、例えばハイパーテキストのリンク

に再びこのゲートウェイ装置1をアクセスしてから、そのゲートウェイ装置1からもとのリンクの指していた先にアクセスするように書いておけば、クライアントを使うユーザがこのリンクを選択すると自動的にこのゲートウェイに再びアクセスするようになる。

【0027】図3は、ゲートウェイ装置1のハイパーテキスト変更装置の説明図である。ハイパーテキスト変更装置4には、リンク置き換え処理装置41とリンク変更処理装置42が設けてある。

10 【0028】以下、このハイパーテキスト変更装置4がハイパーテキストを入力として受け取った時の説明をする。まず、リンク置き換え処理装置41がハイパーテキストを受け取る。リンク置き換え処理装置41は、ハイパーテキストからリンクを抽出し、それをリンク変更処理装置42に渡す。リンク変更処理装置42は、予め与えられた処理方法に従ってリンクを変換し（例えば、このゲートウェイ装置1にアクセスするように変換する）、変更後リンクをリンク置き換え処理装置41に与える。

20 【0029】リンク置き換え処理装置41は、ハイパーテキスト中の元の抽出されたリンクを変更後のリンクに置き換え、最終的に得られたハイパーテキストを出力する。図4は、ゲートウェイ装置のハイパーテキスト化装置の説明図である。ハイパーテキスト化装置5には、ハイパーテキスト化処理装置51とリンク設定処理装置52が設けてある。

30 【0030】以下、ハイパーテキスト化装置5が取得情報を入力として受け取った時の説明をする。ハイパーテキスト化処理装置51が例えば、FTP、GOPHERなどの形態の情報であるいろいろな形態の取得情報を受け取る。そして、リンク以外の部分は通常の方法でハイパーテキスト化する。リンクの部分の生成する段になると、ハイパーテキスト化処理装置51は、リンク設定処理装置52に必要な制御信号（情報）を与える。

40 【0031】リンク設定処理装置52は、予め与えられた処理方法に従ってリンクを生成し、ハイパーテキスト化処理装置51に与える。これによりハイパーテキスト化処理装置51は、そのリンクを通常の方法でのハイパーテキストに統合し、最終的に得られたハイパーテキストを出力する。

【0032】例えば、上記取得情報が、
（プロトコルA+サーバA+付加情報）

であるとする、このリンク設定処理装置52で、このゲートウェイ装置1にアクセスするように書き換える場合は、

プロトコル+このゲートウェイ+（プロトコルA+サーバA+付加情報）

のようにリンク情報を付加する。

50 【0033】この付加したリンク情報は、クライアントのユーザからは隠されているのでユーザには見えない。

従って、ユーザは、外部のネットワーク上でクライアントを動かしているのと全く同様に、組織内部のネットワークから外部のネットワークの各種サーバに自由にアクセスできるように見える。

【0034】図5は、本発明の実施例のフローチャートである。以下、図5のフローチャートに基づいてゲートウェイ装置1の動作を説明する。S1～S9は処理番号を示す。

【0035】まず、アクセス監視・制御装置6がクライアントからアクセスがあるかを調べる(S1)。クライアントからアクセスがあるとアクセス監視・制御装置6は、リンク情報を受け取りリンク解析装置2に渡す(S2)。リンク解析装置2は、アクセス情報を取り出して各種ネットワークサービスアクセス制御装置3に渡す(S3)。各種ネットワークサービスアクセス制御装置3は、アクセス情報を元に指定された情報をネットワーク制御装置7を通して取得する(S4)。

【0036】各種ネットワークサービスアクセス制御装置3は、取得情報がハイパーテキストかどうかを判断する(S5)。この取得情報がハイパーテキストであれば(Yes)各種ネットワークサービスアクセス制御装置3は、ハイパーテキスト変更装置4に取得情報(ハイパーテキスト)を渡し、ハイパーテキスト変更装置4でリンクを予め与えられた処理に従って変更する(S6)。もし、処理番号S5で取得情報がハイパーテキストでなければ(No)各種ネットワークサービスアクセス制御装置3は、ハイパーテキスト化装置5に取得情報を渡し、ハイパーテキスト化装置5は、通常生成されるリンク情報を予め与えられた処理に従って変更してハイパーテキストを出力する(S7)。

【0037】前記処理番号S6、またはS7で処理されたハイパーテキストがアクセス監視・制御装置6に渡される(S8)。アクセス監視・制御装置6がハイパーテキストをネットワーク制御装置7を通してクライアントに返す(S9)。

【0038】図6は、実施例におけるサーバアクセス説明図である。以下、図6に基づいて説明する。図6において、外部のネットワーク12には、ゲートウェイ装置1a、1b、サーバ20～22が設けてあり、組織内部のネットワーク11には、ゲートウェイ装置1c、コンピュータ14、サーバ23、24が設けてある。ルータ15は、組織内部のネットワーク11と外部のネットワーク12を接続しており、例えば、TELNET、FTP、HTTP等の限られたプロトコルしか通れないものである。

【0039】ユーザ13がセキュリティを保ったまま組織内部のネットワーク11上にあるコンピュータ14から外部のサーバ20へアクセスするためには、外部のネットワーク12にゲートウェイ装置1aを置く。更にルータ15は、通常許しているプロトコル(例えば、TE

LNET、FTP)に加えて、例えばハイパーテキストをやりとりするプロトコルであるHTTPのプロトコルを組織内部のネットワーク11の方から通ることを許すようにしておく。

【0040】これにより、一度このゲートウェイ装置1aを通じて外部のネットワーク上にあるサーバ20のリソースにアクセスすれば、アクセスした結果は全てハイパーテキストで返され、リンクは全て再びこのゲートウェイ装置1aにアクセスするように設定される。以後このアクセス過程を何度繰り返してもリンクがこのゲートウェイ装置1aにアクセスするように設定されているので、クライアントのユーザ13がリンクを選択するとこのゲートウェイ装置1aにまずアクセスするようになる。

【0041】また、外部のネットワーク12にこのようなゲートウェイ装置1aをいくつか設ける(例えばゲートウェイ装置1b)場合には、それらのゲートウェイ装置1a、1bを適当な方法で選択してリンクに書き込めば、それらのゲートウェイ装置1a、1bの間で負荷分散することも可能となる。

【0042】例えば、元のリンクの指す先を解析してその指す先に近いゲートウェイ装置を選択する。ゲートウェイ装置1aの負荷によって他のゲートウェイ装置1bに回すようにする。適当に(例えば乱数により)ゲートウェイを選択する。更に、ゲートウェイ間の通信によって負荷の少ないゲートウェイ装置に回す等の方法で行う。

【0043】更に、セキュリティを確保するためだけのゲートウェイ装置でなく、次のようにしても実施可能である。同じネットワーク上のリソースがいくつかの場所にある(例えばサーバ23、24)場合や、ネットワーク上のリソースに別名がついている場合など、それらの情報を貯めておき、ゲートウェイ装置でリンクを書き換える際にそれらを使って書き換えることもできる。

【0044】例えば、同等のネットワーク上のリソースがサーバ23、24にある場合は、適当に負荷を分散するように書き換える。また、外部のネットワーク12上のリソースと同等のリソースが内部のネットワークにある場合には、リンクを内部のリソースを指すように書き換えてしまうこともできる。

【0045】このように、ユーザはリソースに効率のよいアクセスが可能となる。以下、本発明のサーバアクセスを具体例で説明する。まず、WWWにおけるURLを説明する。URL(Universal Resource Locator)とは、情報のありかを示すものである。これは三つの部分からなっており、以下にURLの具体例を示す。

【0046】

http://www.is.university.ac.jp/welcome.html

最初の「:」までの部分(この場合は「http」)はそのサーバへのアクセス方法を示す。この場合はWWWのプ

ロトコルであるHTTP (Hyper Text Transfer Protocol) である。

【0047】次の「:/」と「/」の間はサーバの名前を示す。この場合は指定された情報が「www.is.university.ac.jp」というマシンにあることを示している (なお、この部分でさらにサーバのどのポートにアクセスすればよいのかの情報が与えられる時もある)。残りの部分はそのサーバでの情報のパス (path) が示される。この例の場合では「welcome.html」である。

【0048】図7は、サーバアクセスの具体例の説明図であり、WWWのゲートウェイの例を示す。この例では、組織内部 (社内) のネットワーク11にコンピュータ (クライアント) 14があり、外部 (社外) のネット*

http://www-out.company.co.jp/http://www.is.university.ac.jp/welcome.html

クライアント14は、このURLを解釈し、HTTPでマシン名「www-out.company.co.jp」のゲートウェイ装置1にアクセスする。ルータは、社内のネットワークから特定のプロトコルで社外のネットワークの特定のマシンにアクセスできるように設定されている。この場合のルータ15は、HTTPを通すように設定しているのでクライアント14はゲートウェイ装置1のマシンに到達することができる。そしてクライアント14はゲートウェイ装置1のマシンに対してパスとして「http://www

*ワーク12に直接つながったゲートウェイ装置1のマシンがあり、社外と社内のネットワークはHTTPを通すルータ15でつながっている。このゲートウェイ装置1のマシンの名前を仮に「www.out.company.co.jp」とし、社外のネットワーク12にはHTTPのサーバ25、26とFTPのサーバ27が設けてある。

【0049】最初にユーザ13はURLとして「http://www.is.university.ac.jp/welcome.html」をもつある大学情報科学科のホームページにアクセスしたいと思ったとする。この時ユーザ13は、まず通常のURLの代わりに次のようなURLをクライアント14に対して指定する。

【0050】

w.is.university.ac.jp/welcome.html」を示す。

【0051】ゲートウェイ装置1のマシンはその与えられたパスを元にHTTPでサーバ25 (サーバ名「www.is.university.ac.jp」) にアクセスしに行く。このゲートウェイ装置1は社外のネットワーク12に直接接続しているので問題なくそれらのマシンにアクセスできる。そして、このゲートウェイ装置1は情報として、以下のような情報をもらってくる。

【0052】

```
<HTML>
<HEAD>
<TITLE>
Welcome Message (ABC Univ—Dept Info Sci)
</TITLE>
</HEAD>
<BODY>
<H1>
Welcome to ABC University <p>—Department of Information Science.
</H1>
Welcome to our WWW server!—This is under development, though.
<P>
This WWW server is run by Department of Information Science,
ABC University (somewhere-cho, ABC,
<A HREF="http://www.xyz.jp/japan/index.html">Japan</A>),
which is a new department
established in 1990.
We have a collection of images on the
Earth's environment (in preparation) and
<A HREF="/FTP/images/sat/">
weather information</A>.
We also serve
<A HREF="/FTP/images/sat/gms.polar/">
GMS (Himawari) images </A>
for Chugoku/Shikoku area.
<P>
```


</BODY>

</HTML>

なお、上記<HTML>は、HTML (Hyper Text Markup Language) の形式で書かれた文書の始まりを示し、</HTML>は、その終りを示す。<HEAD>は、文書のヘッダの始まりを示し、このヘッダにはタイトル名やオーサ名などがあり、ここではタイトル名が書かれており、</HEAD>はヘッダの終りを示す。<TITLE>は、タイトルの始まりを示し、</TITLE>は、タイトルの終りを示す。<BODY>は、文書の本文を示し、</BODY>は、その終りを示す。<H1>は、セクションのレベル1の始まりを示し、</H1>

<HTML>

<HEAD>

<TITLE>

Welcome Message (ABC Univ—Dept Info Sci)

</TITLE>

</HEAD>

<BODY>

<H1>

Welcome to ABC University <p>—Department of Information Science.

</H1>

Welcome to our WWW server!—This is under development, though.

<P>

This WWW server is run by Department of Information Science,

ABC University (somewhere-cho, ABC,

Japan),

which is a new department
established in 1990.

We have a collection of images on the
Earth's environment (in preparation) and

weather information.

We also serve

GMS (Himawari) images
for Chugoku/Shikoku area.

<P>

</BODY>

</HTML>

このように変更された情報がゲートウェイ装置1からクライアント14に渡される。クライアント14側では、この情報を例えば図8のようにユーザ13に対して表示する。ここで注意して欲しいのは、書き換えられたリンクの情報はユーザ13から隠されるので、サーバから直接情報をもらった場合も、ゲートウェイを通して情報をもらった場合もユーザ13に対する表示は全く同じであ

*1>は、その終りを示す。<P>は、パラグラフ（段落）の始まりを示しており、この終りは特に必要でない。

【0053】ゲートウェイ装置1は、もらってきた情報と今アクセスしているページの情報を元にリンクである「...」の情報をハイパーテキスト変更装置4で書き換えることにより、以下のように上の情報を変更する。

【0054】

ることである。即ち、上記二つのハイパーテキストをクライアント14は同じに表示することになる。

【0055】ここでユーザ13が例えば、一番最初のリンクである「Japan」をマウス等でクリックすれば、クライアント14に対してURLとして「http://www-out.company.co.jp/http://www.xyz.jp/japan/index.html」を指定したことになり、上と全く同じサイクルが繰

り返される。

【0056】社外のアクセス先がHTTP以外のサーバである場合（例えばFTP, GOPHER）にも同じように書き換えが行われる。例えば以下のようなFTPの*

http://www-out.company.co.jp/ftp://ftp.uvw.edu/gutenberg/etext93/pimil10.txt

このことにより、社内のクライアント14から社外のゲートウェイ装置1のマシンへはHTTPでアクセスが行われる。社外のゲートウェイ装置1のマシンからはFTPで社外のサーバ27へアクセスが行われる。ゲートウェイ装置1のマシンはFTPで得た情報をハイパーテキストに変換し、HTTPでクライアントにその情報を返す。当然上のハイパーテキストの変換では再びそのゲートウェイ装置1にアクセスが行われるようにリンクが書かれている。

【0058】また、ユーザ13がゲートウェイ装置1を通して社外のサーバ27にアクセスし、サーバ27に例えば「Mac・Unix・X11」等のファイルがあった場合、ゲートウェイ装置1は、ハイパーテキスト化装置5でハイパーテキストに変換して、HTTPでクライアント14にその情報を返す。

【0059】この場合、クライアント14は、ユーザ13に対して「Mac・Unix・X11」のリンク表示をすることになり、当然この場合も再びゲートウェイ装置1にアクセスが行われるようにリンクが書かれている。

【0060】

【発明の効果】以上説明したように、本発明によれば直接組織内部のネットワーク上のコンピュータから通常のハイパーテキストのクライアントを使って、セキュリティを犠牲にすることなく、外部のネットワークにある

*サーバ27にある情報のURLの場合には

ftp://ftp.uvw.edu/gutenberg/etext93/pimil10.txt

次のように書き換えられる。

【0057】

リソースにアクセスできるようになり、作業の効率向上を行うことができる。

【図面の簡単な説明】

【図1】本発明の原理説明図である。

【図2】実施例におけるゲートウェイ装置の構成図である。

【図3】実施例におけるハイパーテキスト変更装置の説明図である。

【図4】実施例におけるハイパーテキスト化装置の説明図である。

【図5】実施例におけるフローチャートである。

【図6】実施例におけるサーバアクセス説明図である。

【図7】実施例におけるサーバアクセスの具体例の説明図である。

【図8】実施例における表示画面の説明図である。

【図9】従来例1の説明図である。

【図10】従来例2の説明図である。

【符号の説明】

- 1 ゲートウェイ装置
- 2 リンク解析装置
- 3 各種ネットワークサービスアクセス制御装置
- 4 ハイパーテキスト変更装置
- 5 ハイパーテキスト化装置

【図8】

表示画面の説明図

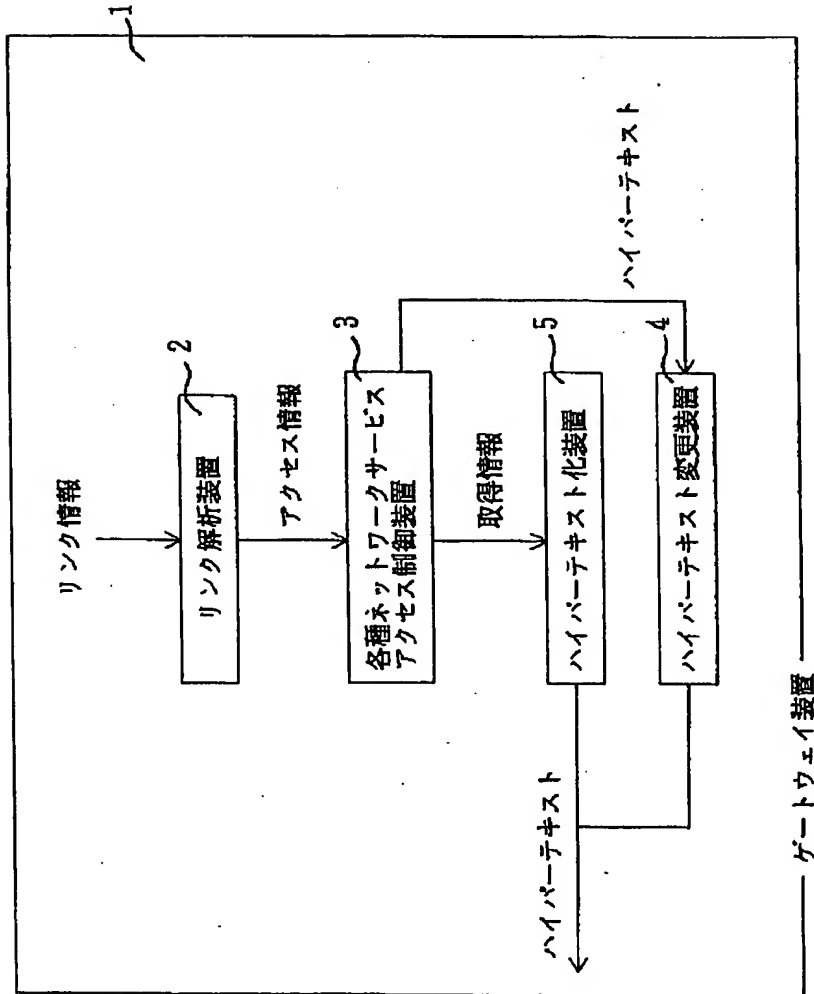
```

Welcome to ABC University
--Department of Information Science.
Welcome to our WWW server!—this is under development, though.

This WWW server is run by Department of Information Science, ABC University
(somewhere-cho, ABC, Japan), which is a new department established in 1990. We have
a collection of images on the Earth's environment (in preparation) and weather
information. We also serve SIGS (Iizawari) images for Chugoku/Shikoku area.
  
```

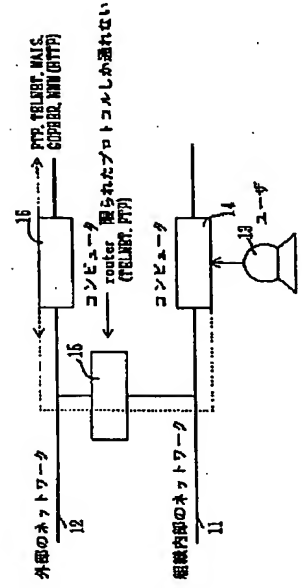
【図1】

本発明の原理説明図



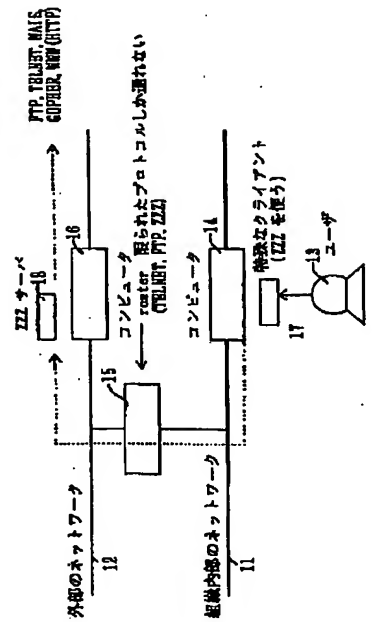
【図9】

従来例1の説明図



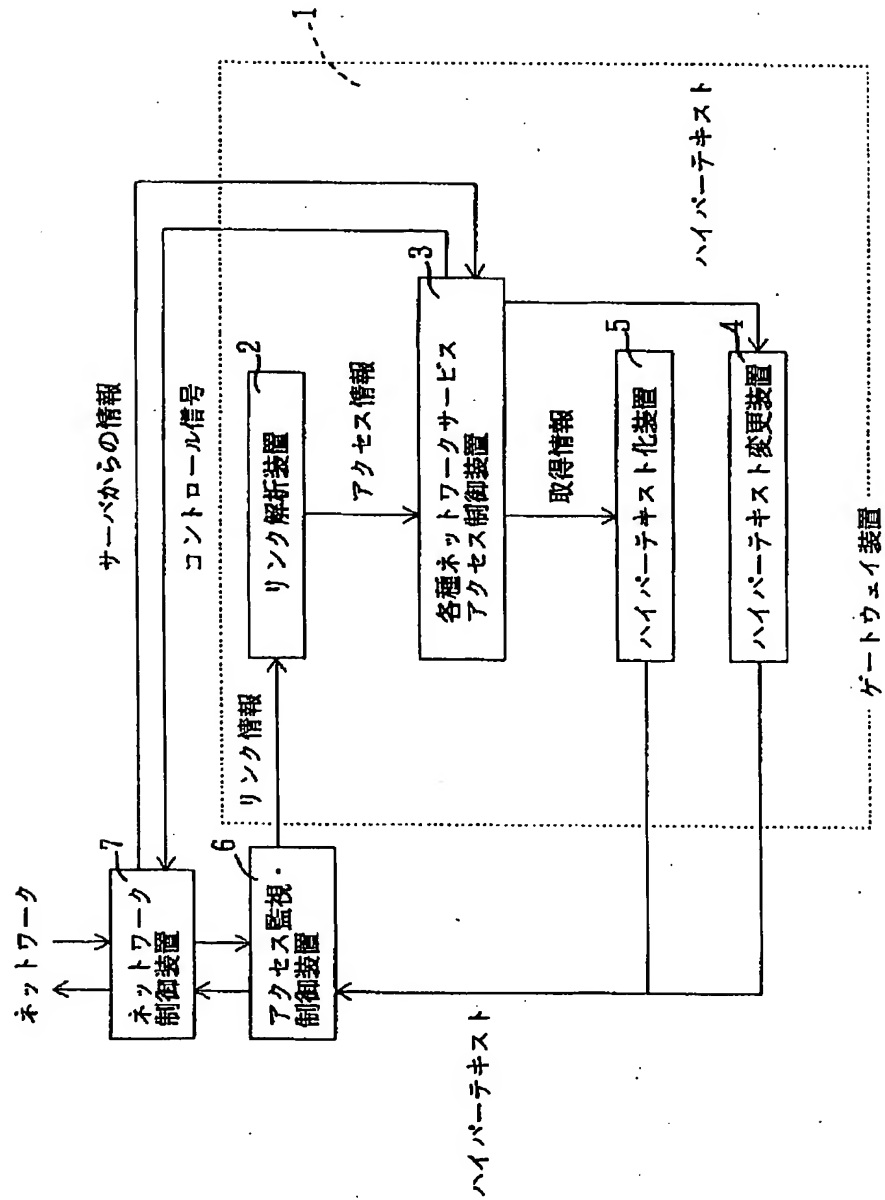
【図10】

従来例2の説明図



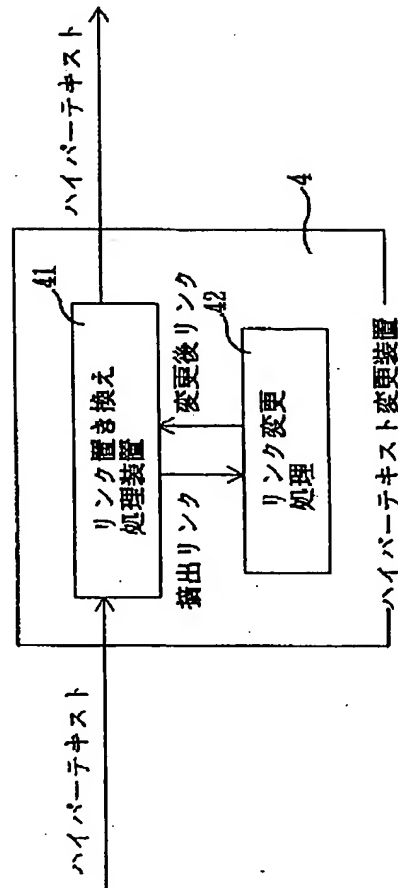
【図2】

ゲートウェイ装置の構成図



【図3】

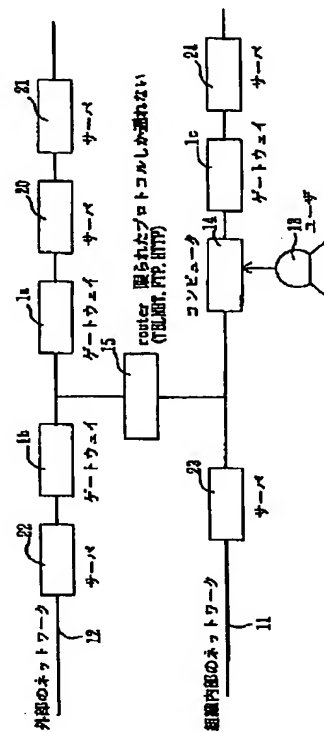
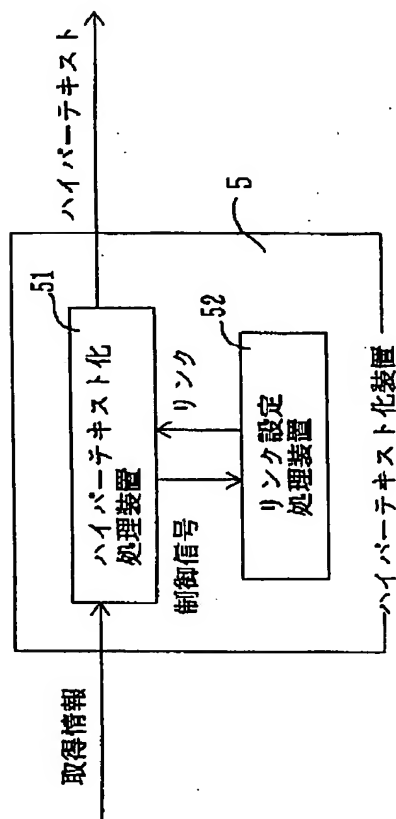
ハイパーテキスト変更装置の説明図



【図4】

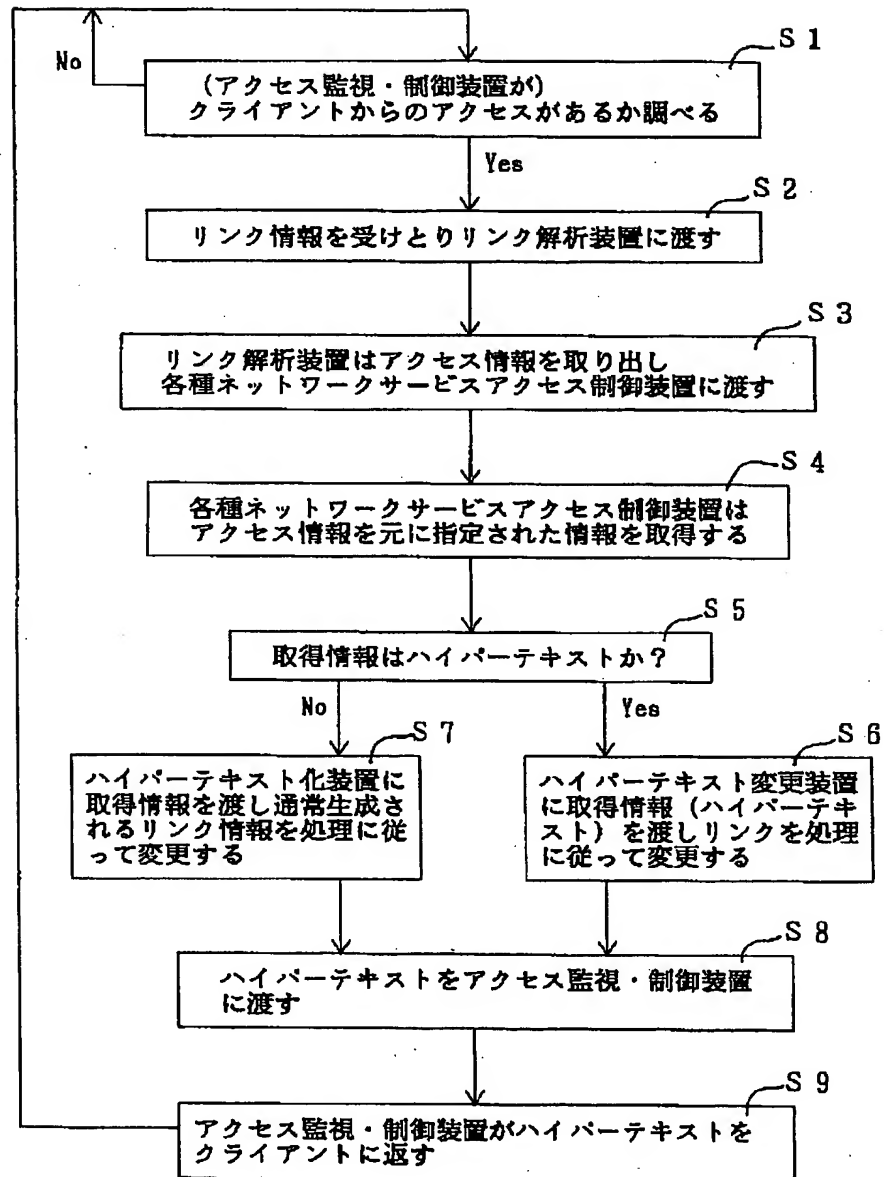
【図 6】

ハイパーテキスト化装置の説明図 実施例におけるサーバアクセス説明図



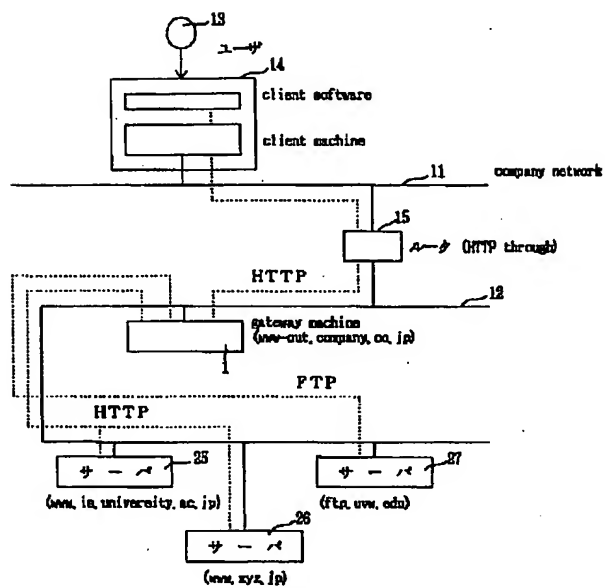
【図5】

実施例におけるフローチャート



【図7】

サーバアクセスの具体例の説明図



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.